BY ORDER OF THE COMMANDER **AFSOC PAMPHLET 31-1**
HQ AIR FORCE SPECIAL OPERATIONS COMMAND **1 December 1996**

Security

SECURITY AWARENESS TRAINING

This pamphlet serves as the standardized lesson plan for Phase I of the command's physical security awareness training program and should be supplemented by security police and unit-appointed phase I/II training officials to fit unit needs. The supplement should include, but are not limited to, specific restricted area entry controls, methods individuals may use to gain unauthorized entry, and a description of the local threat. The blank spaces throughout the text must by filled in, as appropriate, to meet individual base situations.

SUMMARY OF REVISIONS
This revision adds current Human Intelligence (HUMINT) information (para 3), and changes para 4.3.1.1., 5.2.1.1., and Chapter 7.1. to further clarify the subject.

Supersedes AFSOC PAMPHLET 31-1, 1 February 1995.
Certified by: HQ AFSOC/SPO (SMSgt Greg A. Hollingsead)
OPR: HQ AFSOC/SPOS (MSgt Kevin A. White)
Pages: 17
Distribution: F

1. **Introduction:**

- Welcome to _____. In keeping with Air Force policy regarding security education and in compliance with AFI 31-101, chapter 5, as supplemented, the following orientation is designed to introduce you to the AFSOC Physical Security Program and to point out individual responsibilities. To understand what these responsibilities are, we will first discuss the general concept of the program and security threats that confront us. We will then examine the security reporting/alerting system, how to control entry, individual responsibilities, and finally the Installation Security Plan 31-101.

2. **Security Program Concept:**

2.1. Purpose. The Air Force Physical Security Program is designed to deter espionage and hostile activities against Air Force priority resources. This degree of deterrence is achieved by conducting security operations which present hostile persons or groups with unacceptable risks and penalties if they attempt to breach the security system.

2.2. The System. The ideal system to present this unacceptable threat to hostile persons would be to erect barriers and close circuit television that cover 360 degrees, post security police on all resources and install electronic sensors to detect unauthorized entry. However, there aren't enough security police or allocated funds to do this economically. So, security of our resources is a shared responsibility. All personnel who work inside or around a restricted area must support the security effort by being the "eyes" and "ears" for security. To do this, each individual must have knowledge of the "why" and "hows" of security within their specific areas. Additionally, not every piece of material and equipment can be secured in the same manner; there just aren't enough resources to go around. So, resources are prioritized using a security priority system.

2.3. Security Priority System. This system identifies critical resources that you must secure and indicates the amount of security effort you should dedicate to those particular resources. The Security Priority System recognizes that owners and users of such resources must accept a varying degree of risk. The three priorities used in the system are A, B, and C.

2.3.1. What the assigned priority reflects is:

2.3.1.1. What the impact to national defense would be should the resources be damaged or destroyed.

2.3.1.2. The uniqueness and cost of the critical resource.

2.3.1.3. The level of threat to the resource.

2.3.2. Priority Assignments.

2.3.2.1. Priority A is assigned to those resources for which loss, destruction, misuse, or compromise would gravely harm the critical capability of the United States (US) or when the

resources are politically and militarily critical to the US. The Priority A resources on the installation are:

_____

_____

2.3.2.2. Priority B is assigned to non-nuclear alert forces, and high value, limited number, or one-of-kind systems or facilities. Loss, theft, destruction, misuse, or compromise of such resources would likely cause great harm to the warfighting capability of the US. The Priority B resources on the installation are:

_____

_____

2.3.2.3. Priority C is assigned to non-alert resources which can be generated to alert status. Loss, theft, destruction, misuse, or compromise of such resources would damage US warfighting capability or could compromise the defense infrastructure. The Priority C resources on the installation are:

_____

_____

3. **The Threat:**

3.1. There are four Human Intelligence (HUMINT) basic security threats which the enemy can use. Each threat has a singular purpose aimed at causing our downfall. The enemy has a history of experience in all four tactics and is fully aware of how to apply them to their advantage. You have heard them mentioned at one time or another, but let us examine each one and see how they can be employed to achieve maximum results.

3.1.1. The first threat is **espionage** -- the professional use of people to collect information not normally available through legal or authorized channels. Information of a political, economic, social, or military significance is gathered and used against a country in order to eventually defeat it. Spying and the spy have been the subject of glamorized fiction for so many years that the average person sometimes discounts espionage as a real threat. However, it does exist. With the arrest of John Walker in May 1985, "The Year of the Spy" was announced. While spying for the Russians for a shocking 18 years, he recruited his older brother, his best friend, and even his own son to participate in what the government later described as, "The most damaging spy ring in

America's history." After Walker's arrest, the Justice Department went to unprecedented lengths to reveal the damage caused by the

spy ring -- at one point calling upon a high-ranking KGB defector, who described the Walker ring as, "The greatest case in KGB history. We deciphered millions of your messages. If there had been a war, we would have won." Espionage cases like discussed above continue to haunt America. In October 1996, a naval nuclear power instructor was caught attempting to sell military secrets to Russia. Fortunately, he was apprehended before the secrets were disclosed. All countries are engaged in collecting and evaluating military, scientific, and economic information at this very moment.

3.1.1.1. Techniques used to gain information include searching of personal effects, bribery, blackmail, use of electronic listening devices, and elicitation -- the art of finding out information through questions that seem harmless. Elicitation is normally conducted through casual social contact. Most of the above techniques are self-explanatory, but because of its capabilities, additional information concerning electronic devices is warranted.

3.1.1.2. Electronic Devices: Scientific advancements in the field of communications have increased the threat of eavesdropping. Ingenious electronic devices leave virtually no place safe. The use of a microphone set in a reflector, aimed with telescopic equipment can pick up conversations 300 yards away. Miniature radio transmitters, with the invention of the transistor, have been reduced to the size of a wrist watch. Their signals can be received miles away under favorable conditions. Miniature wire and tape recorders, slightly larger than a package of cigarettes, can record up to 2 1/2 hours of conversations. Give a trained agent a few minutes alone in a "secure" office and the agent can convert the office telephone into a listening device that works even when the receiver is in its cradle. These new developments in eavesdropping reveal the seriousness of the threat.

3.1.2. The second threat is **subversion**. Subversion is any activity where individuals willfully attempt to interfere with or impair the loyalty, morale or discipline of any member of the Air Force. It is often so subtle that it is difficult to recognize. Members of the Armed Forces are a primary target for subversion activities because of the key role they play in furthering

national objectives. Through propaganda, rumors, falsehoods, and distortions of the truth, the enemy seeks to create doubt and distrust in the minds of US fighting personnel -- doubts as to the rightness of the cause for which they fight, and distrust of the

abilities and motives of their leaders. By this means, the enemy hopes to destroy, or at least impair, the efficiency of our Armed Forces. Enemy agents are particularly alert to emphasize minor military injustices, discord between the military and civilian population, and trivial incidents of dissatisfaction. The objective is to destroy Air Force esprit de corps. Rumors are one method of accomplishing this. Rumors are used to create fear and destroy confidence. Fear is contagious. The technique of creating fear and panic with rumors is usually more effective under wartime conditions. Trained agents have been very effective with this method of subversion; entire cities have been thrown into an uproar by a single rumor.

3.1.3. The third security threat is **sabotage**. Sabotage is any act committed by any person for the purpose of destroying or hindering the warmaking capability of the United States. This could be accomplished by terrorist, extremist groups, mentally disturbed persons, or even disgruntled military members. There are many ways to commit sabotage and presently known methods may be replaced with new methods and devices. In general, physical sabotage may be accomplished by mechanical means, explosive devices, or arson.

3.1.3.1. Mechanical. Mechanical sabotage covers a wide range of destructive acts. Some of the more common acts are breaking equipment, putting abrasive in moving parts of machinery, contaminating food and water, substituting faulty materials, and acts of omission. The most probable acts are puncturing the skin of pressurized aircraft or missiles with high-powered rifle from off-base, and scattering tire-puncturing material on the runway from light, low flying aircraft.

3.1.3.2. Explosive. Sabotage by explosives simultaneously achieves at least partial destruction of the target, and the initial damage may be followed by fire. Certain explosives can be molded to look like innocent, every-day items (suitcase, package, book, radio, light bulb, etc.) and can be carried inconspicuously to or near the target. They are usually detonated by a timing or trigger mechanism. Timing mechanisms are usually activated by a

clock mechanism, and trigger mechanisms by some normal action, such as picking up the object, opening the package or lid, or turning on a light switch.

3.1.3.3. Arson. The malicious use of fire is one of the oldest methods of saboteurs. It is effective because it can result in

destruction of the evidence as well as complete destruction of the objective. Improvising an arson device is exceedingly simple. Materials are readily available, and their possession, in moderate quantities, does not ordinarily arouse suspicion. Devices can be concealed in soap, cigarette packs, pencils, fountain pens, etc. A book of matches triggered by a lighted cigarette is a simple device which allows the saboteur time to leave the scene.

3.1.4. The fourth security threat is **terrorism.** Terrorism is the use of force or violence, or the threat to use force or violence to accomplish political goals by instilling fear in people. It can include holding hostages that terrorist hope to trade for something they want, or to demoralize US troops as in the June 1996 Khobar Towers bombing in Saudi Arabia. A key note to remember is that terrorist will strike US personnel and facilities in addition to sabotaging operational resources. Furthermore, don't be lured into thinking all terrorist are Middle Eastern in descent. Terrorist come from all cultures and countries as indicated in the 1994 Oklahoma City Federal Building bombing and continued acts of terrorism carried out in Northern Ireland. And finally, one must realize countries who are weak militarily may result to terrorism as their last means of obtaining political objectives. This can best be seen in the current Israeli-Palestinian confrontation.

3.2. What can you do to minimize these threats?

3.2.1. Be fully aware of the enemy's aims, objectives, and subversive techniques.

3.2.2. Abide by established Force Protection measures whether assigned stateside or overseas. Obtain an updated Force Protection briefing from the Office of Special Investigations (0SI) or security police prior to deploying outside of the CONUS.

3.2.3. Develop a sense of personal dedication to national policy and strive to detect when propaganda is used sway your loyalty.

3.2.4. Report to and discuss with your supervisor any activity which appears to be subversive.

3.2.5. Employ entry and internal control of personnel within your restricted area.

3.2.6. Decide what written material needs protection and assign it the proper classification(s).

3.2.7. Establish control systems to ensure that only those who have a **NEED TO KNOW** have access to classified material to perform their duties. Physical safeguards, such as safes, fences, lights, and anti-intrusion alarms are but a few of the devices we employ to hinder espionage activities.

3.2.8. Know the security procedures that apply to your duty area. When in doubt on any security policies, contact your immediate supervisor.

3.2.9. Don't be gullible. Know that enemy agents have an assorted bag of tricks and ruses to gain entry into an area. One method is the use of impersonations. A person may look, talk, and act like a bona fide officer or airman, telephone repair personnel, or fire inspector, but in reality that fast talker may be an enemy agent.

3.2.10. Check all persons in your duty area for proper identification (badge and proper number designator).

3.2.11. Be on guard for the possible use of force to gain entry into an area.

3.2.12. When a hostile or possible hostile event occurs, call the Security Police Control Center (SPCC), (ext_____ or 911), or flag down the security force. **DON'T HESITATE.**

3.2.13. Know your security reporting and alerting procedures.

3.3. Our mission is weakened as long as our base is vulnerable to clandestine activities, such as sabotage, espionage, and

subversion. This weakness can only be eliminated by **YOUR** active participation in our security system. But to do this you must have some knowledge of the local threat:

_____

_____

_____

_____

4. **The Security Reporting and Alerting System:**

4.1. An integral part of the Aerospace System Security Program is the Security Reporting/Alerting System. This section will acquaint you with the system and your responsibilities.

4.2. Purpose of the System:

4.2.1. A rapid security communications procedure that integrates all USAF bases and commands through a series of up-channel and down-channel reports. By this system, a significant happening at one location or a pattern of seemingly unrelated happenings at several locations can serve as a basis for swift security alerting or warning throughout the USAF.

4.2.2. It provides for the earliest possible indication of enemy clandestine operation at its onset. We can then capitalize on any error made by the enemy in their timing of widespread coordination of clandestine operations against individual bases.

4.3. Reports and Conditions. How do we keep personnel at all levels informed of activities affecting the security of our resources? Up-channel reports, threat conditions, and down-channel reports. These reports and conditions are given nicknames and are the backbone of the Security Reporting/Alerting System.

4.3.1. Up-Channel Reports. The two types of up-channel reports used to alert command centers of hostilities (possible or actual) are nicknamed **HELPING HAND** and **COVERED WAGON.**

4.3.1.1. HELPING HAND. This is an unclassified message relayed by SPCC to the installation command post informing them that an unusual incident, possibly hostile and affecting priority resources, has been detected. Incidents are reported to the SPCC

by any means available by anyone who witnesses or discovers the problem.

4.3.1.1.1. This report is not immediately relayed to higher headquarters, because it reflects a situation not completely investigated.

4.3.1.1.2. The incident must be investigated by security force personnel. The security team must determine if the event is hostile or not. It may turn out that the incident is a procedural violation (e.g., an individual failing to wear a restricted area

badge) in which case the HELPING HAND would be canceled. However, the violation will not go unnoticed. It is possible the person will be cited on DD Form 1569, Incident/Complaint Report, for violation of Article 92, UCMJ, which requires the commander to take action. If the situation is determined to be hostile, the HELPING HAND Report must be upgraded to a COVERED WAGON.

4.3.1.2. COVERED WAGON. This is an unclassified upchannel telephone report (designator immediate or flash) sent up the same communication channel and in the same format as a HELPING HAND report. COVERED WAGON reports informs higher headquarters that an unusual incident, probably or actually hostile, affecting priority resources has occurred at an installation or dispersed site.

4.3.1.2.1. A COVERED WAGON Report could result as an upgrading of a HELPING HAND, based on investigation by security forces. It could also result if an event is serious enough to immediately suspect enemy action (e.g., sudden explosion which destroys an aircraft).

4.3.2.2.2. When a COVERED WAGON is declared, increased security measures, specifically Threat Condition **(THREATCON)** Delta will be implemented.

4.3.2. THREATCONs. THREATCONs are the standard terms used to identify the security posture of each installation. There are a total of five conditions that can be implemented by the installation commander or higher authority. Each condition has its own actions but is designed to build on the actions of a lesser condition. Detailed guidance on actions required under specific THREATCONs can be found in AFI 31-210, MAJCOM supplements, and installation security plans.

4.3.2.1. THREATCON NORMAL: Exists when a general threat of possible terrorist activity exist, but warrants only a routine security posture.

4.3.2.2. THREATCON ALPHA: This condition applies when there is a general threat of possible terrorist activity against installations and personnel and the nature and extent of which are unpredictable.

4.3.2.3. THREATCON BRAVO: This condition applies when an increased and more predictable terrorist threat activity exists, even though no particular target has been identified.

4.3.2.4. THREATCON CHARLIE: This condition applies when an incident occurs or when intelligence is received indicating some form of terrorist action against the installation and personnel is imminent.

4.3.2.5. THREATCON DELTA: This condition applies in the immediate area where there is a terrorist attack or when intelligence has been received that terrorist action against a specific location or person is likely.

4.3.3. Down-Channel Report THREATCON Alerting Message (TCAM). When the number of active reports (up-channel reports) indicate coordinated or widespread hostile activities a down-channel report is used to alert installation commanders of the need to increase their state of readiness. The TCAM is used for this purpose.

4.3.3.1. A TCAM is transmitted electronically by the Air Force Operations Center or MAJCOM Command Center to installations.

4.3.3.2. As a rule, the message will not implement a theater-wide or AF-wide THREATCON, but will provide a synopsis of the situation which led to the release of the message and a recommended course of action. This provides commanders flexibility to tailor their actions (THREATCON implementation) to their local situation. How-ever, if the alerting message mandates a certain THREATCON be implemented, the implementation is mandatory and can only be canceled by the originator.

4.4. Security Reporting/Alerting System in Action: (Scenario)

4.4.1. Scenario:

4.4.1. A sentry or other base member detects what looks like a bullet hole in the wing of an aircraft. They, immediately initiate an alarm to the SPCC, ext_____. This results in an automatic HELPING HAND report to the installation command post.

4.4.2. The Security Response Team is notified and dispatched to the scene to investigate. The investigation supports upgrading the situation to a COVERED WAGON. The installation command post relays the COVERED WAGON report directly to the HQ AFSOC Command Center. The base implements THREATCON BRAVO.

4.4.3. At the AFSOC Command Center, the COVERED WAGON report is received, logged, and evaluated. Other such reports from installations indicate the possibility of wide-spread coordinated hostile activity. A THREATCON Alerting Message is sent to all AFSOC installations describing the incidents and recommending THREATCON ALPHA actions be considered at those locations where incidents have not occurred. Over 75 percent of the installations choose to implement THREATCON ALPHA. Since the alerting message did not mandate THREATCON implementation, the others have chosen to brief the incidents to the base populace and not implement a THREATCON unless the local situation changes.

4.4.4. What is the most essential feature of this system? What factor will enable us to oppose unfolding, widespread, enemy clandestine operations with maximum possible preparedness? In one word--**SPEED**.

4.4.4.1. Speed in which required reports are initiated at base level.

4.4.4.2. Speed in which reports are flashed to and analyzed by higher headquarters.

4.4.4.3. Speed in which higher headquarters re-transmits TCAMs to subordinate installations.

4.4.4.4. Remember, any circumstances delaying the receipt of Helping Hand or Covered Wagon reports will lessen the possibility of timely reaction to the opening phase of a wide-spread coordinated enemy attack.

5. **Control of Entry and Movement of Personnel Within Restricted Areas:**

5.1. The control of entry and internal movement of personnel in restricted areas is an essential part of the security program. Entry and movement of personnel must be limited to only those absolutely required for the performance of official duties and who have been granted specific authority.

5.2. Entry Authority. The two types of entry authority into restricted areas are identified as escorted and unescorted.

5.2.1. Escorted Entry. Visitors having an official need to enter a restricted area, but not on a frequent basis, must be escorted. In these instances, a sponsor (escort official) for the restricted area is requested and must validate the visitor's need to enter the restricted area. The escort official is responsible for the visitors actions while inside the area and must ensure the safe and secure conduct of the visitor.

5.2.1.1. The escort official is identified by having an "E" typed next to the restricted area number on the restricted area badge indicating the area they are authorized to escort personnel. **EXCEPTION:** For restricted areas containing priority C resources, any person having unescorted entry authority for that area may perform as an escort official. An "E" printed next to the open area on the restricted area badge is not required, unless the system security standard dictates otherwise(e.g., command post/centers that are Priority “C”, but require an “E” to escort).

5.2.1.2. The escort official must meet the visitor at the entry control point, verify their identity and need to enter the restricted area and give a briefing on security procedures prior to entry.

5.2.2. Unescorted Entry. Authority is based on the frequency of a person's need to enter the restricted area and personnel security qualifications outlined in AFI 31-501. Those who have unescorted entry are issued a USAF Restricted Area badge (RAB) to facilitate entry control.

5.3. Entry Control and Circulation Controls:

5.3.1. Entry Control. The USAF RAB serves as an official credential issued to personnel who have been granted unescorted entry authority. Each badge is designed with a series of numbers to indicate the particular area for which the person is authorized unescorted entry. In our system at _____, the single -badge procedure is used. By itself, any single-badge procedure can be defeated with relative ease. So with this procedure, at least one of the following supporting identification/verification techniques is used:

5.3.1.1. Personal Recognition -- this is the most reliable, providing the numbers of personal under control are relatively small.

5.3.1.2. Signature and Credential Checks -- a person can be asked to sign their name, recite their SSAN or show an ID card or some other identifying supplemental credential.

5.3.1.3. Entry Authority List (EAL)--this is an authenticated list of names of persons authorized into an area. The EAL is maintained at the entry control point.

5.3.1.4. Telephone or Radio verification with the SPCC.

5.3.2. Duress Codes. In addition to the techniques listed above, a duress code is usually established. A duress code is a predetermined word passed during normal conversation to indicate a duress situation. The duress word is locally established and must be protected against inadvertent disclosure. If you hear the duress word being passed, immediately contact the SPCC at ext_____ to report a duress situation in progress. **DO NOT** alert others in the area that you have contacted the security police, as this may endanger their lives.

5.3.3. Internal Circulation Control. The fundamental objective of an entry control procedure (described above) is to establish the identity of each person who seeks to enter. However, security doesn't stop there; movement within the area must be monitored. This is where internal controls come in. If a saboteur or terrorist is able to penetrate the outer perimeter undetected, the last line of defense is those working within the area **(in other words, YOU).**

5.3.3.1. Be watchful for suspicious or careless acts, and people in the area without a RAB.

5.3.3.2. DON'T be fooled by persons in the area who uses excuses such as, "I forgot my badge" or "It must have fallen off." Be alert; everyone must have a badge or be properly escorted.

5.3.3.3. Internal controls properly affected and supported by you can be extremely effective against clandestine actions. The very purpose of internal controls is to make the interior of a restricted area as hazardous an environment as possible for any unauthorized person.

5.3.4. Security in a restricted area is a cooperative effort. Who would know better if a tug operator is operating the tug in a manner which would damage a mission aircraft than another tug

operator? Who would know if an engine mechanic is properly performing their duty better than another mechanic? No restricted area is intruder proof. We will make it as secure as our system allows, but unauthorized persons may still enter, so your watchfulness is a valuable adjunct to the security effort.

6. **Individual Program Responsibilities:**

6.1. The one basic requirement for everyone is **IMMEDIATE RECOGNITION AND REACTION TO HOSTILE ACTS.** Here are the necessary actions required to effectively control and counter hostile or possible hostile events. It is a simplified effort to explain HOW YOU can meet your security obligation while performing duties in a restricted area.

6.1.1. First and foremost, you must be **ALERT**. Know who and what is going on around you at all times. Be alert for unauthorized personnel in the area. As you approach individuals, look for their RAB. If they have a proper badge and you recognize them, resume your duties. If they have a badge, but are not recognized, check them out further (area number designation, ID card, etc.) and determine that they have authority and an official reason for being in the area. The number required for entry into your area is _____.

6.1.2. **DETECT** hostile acts which could affect our priority resources. Look for any abnormal condition of equipment on which

you work, such as cut wires, improper positioning, visual signs of tampering, etc. Be alert to detect anything that strikes or is cast toward our operational resources.

6.1.3. **ALERT OTHERS** in the immediate area upon detection. Yell **"HELPING HAND"** loud and clear! Make it a spontaneous reaction, like when you touch something hot. Alerting others in the area should bring assistance. If you hear the HELPING HAND alarm, you should temporarily drop what you are doing, safety permitting, and assist. Noise levels or extreme distance may prevent personnel from hearing the alert. In these cases visual signals are necessary. The day and night signals for this installation are:

_____
_____
_____
_____
_____

6.1.4. After alerting others in the area, and if an unidentified person is involved, you are confronted with the twofold task of reporting the incident to SPCC, ext_____ and detaining unauthorized personnel. These tasks might be referred to as the Siamese twins of security, not because they are inseparable, but because they must be accomplished simultaneously, and occasionally in conjunction with each other.

6.1.4.1. If other personnel are immediately available, your tasks become comparatively simple. You get their assistance to detain and remove the unidentified person from sensitive resources in the area. You then run to the nearest telephone or vehicle radio and report the nature and location of the incident to SPCC. If a Security Force is in the area and readily available, attract their attention to the scene.

6.1.4.2. What if no other personnel are available to assist you? The obligation of detaining an unauthorized person and promptly reporting the incident may well be beyond your capability. It may require the accomplishment of one task at the expense of the other. In such instances, you must accurately evaluate comparative physical superiority of the suspect, weapons in their possession, and the extent of damage that they could inflict on our sensitive resources. These considerations must be compared against the time

it will take you to report the incident to the SPCC and receive assistance from the security force. If at all possible, accomplish both tasks simultaneously. If they are obviously beyond your capability, report the incident to the SPCC as rapidly as possible. Stay cool and speak plainly when reporting. Don't omit the **"WHAT"** and **"WHERE"** of your report. These two factors are required in dispatching the help you need.

6.1.4.3. After you make the report, return to the area where the suspect was last seen. Attempt to relocate the suspect and keep this individual under observation. Look for and attract the attention of the security force so it will arrive at the scene at the earliest possible moment. Meet the security force and immediately report the incident again and any other pertinent information you have. Explain what happened. The information which you give the security force is the basis for their necessary counteractions.

6.2. It is no exaggeration when it is said that our combat capability can be placed in unnecessary jeopardy if you fail to carry out your individual security responsibilities to **DETECT** and **REPORT** hostile or possible hostile events, and **DETAIN** (if possible) unauthorized persons.

7.1. **Installation Security Plan (ISP):**

7.1. Purpose. This is the basic planning document for contingency operations. Each base routinely supporting priority resources publishes an ISP.

7.2. What does it contain? There are several annexes and appendices to the ISP. These contain the installation threat analysis (what the local threat is and its impact on the installation) and tasks and responsibilities for organizations during increased (THREATCONs and contingency operations). Every attempt is made to ensure the ISP covers as many scenarios as possible that would affect the operational status of our resources.

8. **Conclusion:**

8.1. The Threat. Be fully aware of enemy aims, objectives, and subversive techniques. Develop a sense of personal dedication to national policy. Report and discuss any activity which appears to be subversive with your supervisor. Our defenses against espionage are many and you perform a vital part in all of them. You can defeat the enemy's attempts at espionage by strictly following a few simple habits of thinking and acting, both on and off duty. Be security conscious every day. Be security cautious every day. Be cautious of new friendships, especially if they are developed out of strange and unexplainable circumstances. Avoid foolish suspicion, report them immediately to your supervisor. Tell no one else.

8.2. Your Role:

8.2.1. Know your security reporting and alerting procedures.

8.2.2. When a hostile or possible hostile event occurs, call the SPCC, or flag down the security force.

8.2.3. Be on guard for the possible use of force to gain entry into your area.

8.2.4. Don't be gullible. Know that enemy agents have an assorted bag of tricks and rules to gain entry into a restricted area. These agents do not advertise their arrival. They may look just like Americans or may even be in the military. They seem to belong, but in fact, they are strangers and it is your responsibility to apprehend these agents. They may have gotten past the security police. They will in most cases, have proper credentials. They will know where and what they are going to do. The only thing that will probably be wrong is that no one seems to know them.

8.2.5. Know the security procedures that apply to your duty area. When in doubt on any security matter, contact your immediate supervisor.

MATTHEW P. BRANIGAN, Lt Col, USAF
Director, Security Police